AMENDMENTS TO THE DRAWINGS:

The sheet, which includes Figures 1 and 2, replaces the original sheet including Figures 1 and 2. The Applicants submit that no new matter has been added by the amendment of Figures.

Attachment: Replacement Sheet

REMARKS

In the Office Action mailed September 16, 2008 the Office noted that claims 22-44 were pending and rejected claims 22-44. Claims 22-41, 43 and 44 have been amended, claim 42 has been canceled, claims 45 and 45 are new, and, thus, in view of the foregoing claims 22-41 and 43-46 remain pending for reconsideration which is requested. No new matter has been added. The Office's rejections and objections are traversed below.

OBJECTION TO THE SPECIFICATION

The disclosure stands objected to for informalities. In particular, the Office states that the Specification lacks headers. The Applicant has amended the Specification to include headers. The Applicant has further amended the Specification to correct translation errors from the foreign priority document.

The Applicant has amended the Specification in compliance with the comments of the Office.

Withdrawal of the objections is respectfully requested.

DRAWINGS

The Applicant has amended drawings 1 and 2 to be better quality drawings and to bring them into conformity with the Specification. The Host computer is now represented as supported in ¶¶ 0034 and 0036 of the printed publication version of the

Specification. The box “Memory Context” has been added to Fig. 2, with support found, for example, in ¶ 0040. In amended figure 1, the arrow 10 has been directed to the software 1, and not to data 2 as in original figure 1. As mentioned in ¶ 0040, the data are processed by the software 1, which means that the signature allows the software to read them. The signature is a data which cannot have any action on other data.

CLAIM OBJECTION

Claims 22-24 and 26-44 stand objected to for informalities. In particular, the Office asserts that the claims use European style transitional phrases. The Applicant has amended the claims to conform with U.S. practice.

Claims 31, 41 and 42 stand objected to for using the and/or type language. The Applicant has amended the claims to overcome the rejection.

Withdrawal of the objections is respectfully requested.

REJECTIONS under 35 U.S.C. § 112

Claims 30, 34-42 and 44 stand rejected under 35 U.S.C. § 112, second paragraph as being indefinite for failing to particularly point out and distinctly claim the subject matter which the applicant regards as the invention. In particular the Office asserts that the claims contain antecedent basis issues and that the means plus function of some of the claims are not supported by the Specification. The Applicant has amended the claims to remove any antecedent basis issues.

The Applicant respectfully submits the “means for” are explicitly or implicitly disclosed in the specification and shown in the drawings by the arrows.

The “means for moving” are implicitly disclosed by the fact that the host terminal is a data processing apparatus, a digital television decoder… or the like. This implies that the moving means are the usual means for downloading information to such devices.

Since the positive comparison of the invention is implicit, the “means for comparing” cannot be disclosed more properly than by their result which is to let the application run without error if the application is authentic ¶ 0014.

The “means for communication” in claim 35 are disclosed in ¶ 0044 and represented by the arrow 12 of figure 2.

The “verifying means” in claim 36 are clearly identified as reference 24 in ¶ 0047.

The “means which are capable of inserting” in claim 44 may be found, for example, in claims ¶ 0039 and 0040.

Withdrawal of the rejections is respectfully requested.

REJECTIONS under 35 U.S.C. § 102

Claims 22-23 and 25-44 stand rejected under 35 U.S.C. § 102(e) as being anticipated by McCarroll, U.S. Patent Publication

No. 2003/0196102. The Applicant respectfully disagrees and traverses the rejection with an argument and amendment.

McCarroll discusses in ¶ 0007 digitally signing a portion of software with a first key (private key) and decrypting the signature with a second key (public key). The signature of McCarroll is not a certificate according to the invention since it cannot be executed and it is not produced in the memory context of the authentic software application and executed in the memory context of the application to be verified.

The comparison of McCarroll is clearly a mathematical one (¶ 0030 makes use of the word "match") and not a positive comparison as defined in the present patent application. If the comparison of McCarrol does not match, the operation of the system is prevented ¶ 0029, whereas the verification of the claimed invention is carried out during the execution of the application software.

McCarroll's method requires a tamperproof circuit 120 for the cryptography operations, whereas the certificate of the invention is executed on the host terminal itself.

In summary, in the invention, the application to be verified and the certificate are readily executable (they are not encrypted) and executed on the host terminal without verification. The verification process takes place during the execution.

In McCarroll, a signature is decrypted before the application is executed. The memory context of the authentic application does not intervene in the process and there is no memory context of the application to be verified since the application is not running.

On pages 6 and 7 it is asserted that McCarroll, ¶¶ 0026 and 0027 disclose "determining at least one series of control instructions forming an executable certificate for the software application, which can be executed by said host terminal during the execution of the software application to be verified."

However, for reasons discussed above, McCarroll does not disclose an executable certificate. To emphasize this distinction, the Applicant has amended claim 22 to recite ***"using the memory context of the authentic software application during the course of execution for*** determining at least one series of control instructions forming an executable certificate for the software application, which can be executed by said host terminal during the execution of the software application to be verified." (Emphasis added) Support for the amendment may be found, for example, in ¶¶ 0018 and 0020 of the printed publication version of the Specification. The Applicant submits that no new matter is believed to have been added by the amendment.

For at least the reasons discussed above, claim 22 and the claims dependent therefrom are not anticipated by McCarroll.

As regards claims 27, the Applicant has amended the term "card" to read "map". Support for the amendment may be found, for example, in ¶ 0018 of the Specification. The Applicant submits that no new matter has been added by the amendment of claim 27. The prior art of record fails to disclose a map of the memory context.

On pages 8 and 9 of the Office Action, it is asserted that McCarroll, ¶¶ 0026-0028 disclose "wherein, in step ii), the recovery of the execution values of the memory context comprising the step of reading the values at the addresses of the various portions of the memory of the host terminal, these portions containing the executable instructions and the data intrinsic to the application to be verified," as in claim 1.

However, the instructions forming the executable certificate are executed in the memory context of the application to be verified (which then has to be executed at the same time) which means that the execution of the application allows the execution of the certificate.

In contrast, in McCarroll the verification is made in a secure part of the host terminal and has therefore no access to the memory context of the application to be verified (which anyway is not running).

There is no memory context in McCarroll since the application is not running during the process of verification, thus, McCarrol does not disclose "wherein in step iii), the result obtained by the execution of said series of control instructions produces a signature for the application to be verified, said step iii) comprising the step of calculating this signature by said series of control instructions which uses the values of the memory context of the software application to be verified during the course of execution of the application," as in claim 29.

As regards claim 30, since the software application to be verified is not running in McCarroll, there in no address for executing instructions and therefore no possibility to substitute such an address by another address.

As regards claim 31, it is respectfully submitted that fraudulently modifying a software application in McCarroll and temporarily modifying (for a positive comparison purpose) the state of the memory context of a software application during its execution are different. As previously stated, there is no memory context in McCarroll.

Withdrawal of the rejections is respectfully requested

REJECTIONS under 35 U.S.C. § 103

Claim 24 stands rejected under 35 U.S.C. § 103(a) as being obvious over McCarroll in view of Yach, U.S. Patent Publication No. 2004/0025022. The Applicant respectfully disagrees and traverses the rejection with an argument.

Yach adds nothing to the deficiencies of McCarroll as applied against the independent claim. Therefore for at least the reasons discussed above, McCarroll and Yach, taken separately or in combination, fail to render obvious the features of claim 24.

NEW CLAIMS

Claims 45 and 46 are new. Support for claims 45 and 46 may be found, for example, in claims 41 and 31. The Applicant submits that no new matter has been added by the addition of claims 45 and 46. The prior art fails to disclose the series of control instructions is selected in such a manner that the state of the memory context of the software application after the execution of the series of control instructions is without any modification to the state of the memory context of the software application prior to the execution of the series of control instructions; or the processing means comprises means for determining a plurality of executable certificates which differ from one another according to a selected condition.

SUMMARY

It is submitted that the claims satisfy the requirements of 35 U.S.C. §§ 112 and 102. It is also submitted that claims 22-41 and 43-46 continue to be allowable. It is further submitted that the claims are not taught, disclosed or suggested by the prior art. The claims are therefore in a condition suitable for allowance. An early Notice of Allowance is requested.

Charge the fee of $26 for the one claim of any type added herewith to our credit card.

The Commissioner is hereby authorized in this, concurrent, and future replies, to charge payment or credit any overpayment to Deposit Account No. 25-0120 for any additional fees required under 37 C.F.R. § 1.16 or under 37 C.F.R. § 1.17.

Respectfully submitted,

YOUNG & THOMPSON

/James J. Livingston/
James J. Livingston, Jr.
Reg.No. 55,394
209 Madison St, Suite 500
Alexandria, VA 22314
Telephone (703) 521-2297
Telefax (703) 685-0573
(703) 979-4709

JJL/fb

APPENDIX:

The Appendix includes the following item(s):

☒ - a new or amended Specification in clean and marked up versions

☒ - replacement drawings